ATTACHMENT B

Things to be Seized

I. Information to be Disclosed by Discord, Inc. ("DISCORD") to Facilitate Execution of the Warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of DISCORD, including any information that has been deleted but is still available to DISCORD, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), DISCORD is required to disclose the following information to the government for each TARGET ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the TARGET ACCOUNT for the period January 1, 2023 through June 1, 2024, including:

i. All e-mails, communications, or messages of any kind associated with the TARGET ACCOUNT, including stored or preserved copies of messages sent to and from the TARGET ACCOUNT, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments;

ii. All records or other information stored by subscriber(s) of the TARGET ACCOUNT, including address books, voice and voice-over-IP data, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files;

iii. All records pertaining to communications between DISCORD and any person regarding the TARGET ACCOUNT, including contacts with support services and records of actions taken;

iv. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, DISCORD shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

v. All search history and web history, including web clicks or "History Events," by the user of the TARGET ACCOUNT;

vi. All web browsing activities that are identifiable with the TARGET ACCOUNT; and

vii. Any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning other e-mail or social media accounts accessed or analytics related to the TARGET ACCOUNT.

b. All other records and information, including:

i. All subscriber information, including the date on which the TARGET ACCOUNT was created, the length of service, the IP address used to register the target account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the target account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers, or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates

and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(1) The TARGET ACCOUNT;

(2) Any other account associated with the TARGET ACCOUNT, including by means of sharing a common secondary, recovery, or alternate **e-mail address listed in subscriber records** for the TARGET ACCOUNT or by means of sharing a **common phone number or SMS number listed in subscriber records** for the TARGET ACCOUNT; and

(3) Any other account accessed by a device with an identifier responsive to the device identifiers called for in Section I.b.iii, below.

ii. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT described above in Section I.a, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations;

iii. Any information identifying the device or devices used to access the TARGET ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC address, Electronic Serial

Number ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifier ("IMSI"), International Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDEFA"), and any other information regarding the types of devices used to access the TARGET ACCOUNT or other device-specific information; and

iv. Any information showing the location of the user of the TARGET ACCOUNT, including while sending or receiving a message using the TARGET ACCOUNT or accessing or logged into the TARGET ACCOUNT.

Within **14 days** of the issuance of this Warrant, DISCORD shall deliver the information set forth above to the FBI as directed.

II. Information to be Seized by the Government

For each TARGET ACCOUNT listed in Attachment A, the search team may seize all information described above in Section I that constitutes evidence, contraband, fruits, or instrumentalities of violations of Title 18, U.S.C § 2251(a) (sexual exploitation of children), 2252A(a)(5)(B) and (b)(2) (possession of and access with the intent to view child pornography), 2252A(a)(2) and (b)(1) (receipt or distribution of child pornography), and related crimes, as described in the Affidavit submitted in support of this Warrant, which is hereby incorporated by reference, including, but not limited to, for each TARGET ACCOUNT, information pertaining to the following matters:

a. Information that constitutes evidence of the identification or location of the user(s) of the TARGET ACCOUNT;

b. Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the TARGET ACCOUNT about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

c. Information that constitutes evidence indicating the TARGET ACCOUNT's user's or his co-conspirators' state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

d. Information that constitutes evidence concerning how and when the TARGET ACCOUNT was accessed or used, to determine the geographic and chronological

context of account access, use, and events relating to the crime under investigation and to the TARGET ACCOUNT's user;

e. Information, including messages, communications, audio recordings, pictures, video recordings, or still captured images, that constitutes possession, receipt, or distribution of child sexual abuse material (CSAM) or cyberstalking, including any conspiracy to do so independently or with the assistance of another person; records showing sexual interest in children including child erotica; messages, communications, audio recordings, pictures, video recordings, or still captured images of V1; or communications and associated data pertaining to the transfer of images of V1.

f. Current and historical friends list, stating all full-case sensitive usernames including the 4-digit discriminator; and

g. List of users the TARGET ACCOUNT have communicated with, to include content of private chats.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by DISCORD in order to locate the things particularly described in this Warrant.